PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-073415
(43)Date of publication of application : 18.03.1997

(51)Int.Cl. G06F 12/14
G06K 17/00
G09C 1/00
H04L 9/10

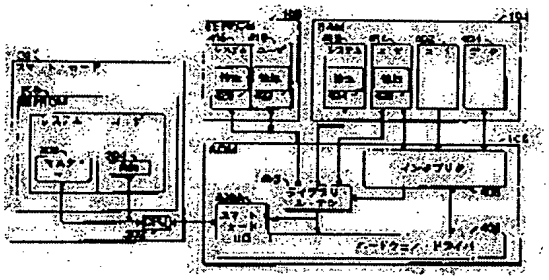
(21)Application number : 08-178188
(22)Date of filing : 08.07.1996

(71)Applicant : THOMSON CONSUMER ELECTRON INC
(72)Inventor : ROHATGI PANKAJ

(30)Priority
Priority number : 95 499170 Priority date : 07.07.1995 Priority country : US

(54) METHOD FOR SAFELY STORING SENSITIVE INFORMATION IN STORAGE MEDIUM WITH RELATIVELY LOW SAFETY DEGREE AND DEVICE THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide method and device safely storing sensitive information in a computer system incuding a storage medium with relatively high safety degree and a storage medium with relatively low safety degree.
SOLUTION: Sensitive information is ciphered by using a cryptographic key 302. Next, the ciphered sensitive information is stored in storage media 108 and 104 with relatively low safety degree and the cryptographic key 302 is stored in a storage medium 208 with relatively high safety degree. By this device, sensitive information is safely stored in the computer system including the storage medium 208 with relatively high safety degree in which the cryptographic key 302 is stored and storage media 108 and 104 with relatively low safety degree. A ciphering device 202 ciphers sensitive information by using the cryptographic key 302 and stores the ciphered sensitive information in storage media 108 and 104 with relatively low safety degree.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－73415

(43)公開日　平成９年(1997)３月18日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　12/14	３２０		Ｇ０６Ｆ　12/14	３２０Ｂ	
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ　17/00	Ｓ	
Ｇ０９Ｃ　1/00	６３０	7259－５Ｊ	Ｇ０９Ｃ　1/00	６３０Ａ	
Ｈ０４Ｌ　9/10			Ｈ０４Ｌ　9/00	６２１Ａ	

審査請求　未請求　請求項の数20　ＯＬ　（全 14 頁）

(21)出願番号　特願平8－178188

(22)出願日　平成８年(1996)７月８日

(31)優先権主張番号　０８／４９９１７０

(32)優先日　1995年７月７日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　391000818
トムソン　コンシユーマ　エレクトロニクス　インコーポレイテツド
THOMSON CONSUMER ELECTRONICS, INCORPORATED
アメリカ合衆国　インデイアナ州　46290－1024　インデイアナポリス　ノース・メリデイアン・ストリート　10330

(72)発明者　バンカジャ　ロハトギ
アメリカ合衆国　94086　カリフォルニア州　サニーヴェイル　ヴィンセント　ドライブ　1256　アパートメント　エイチ

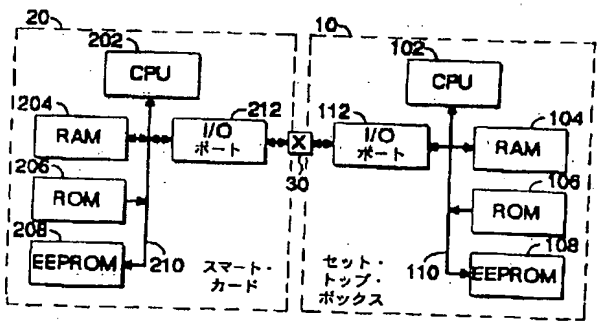
(74)代理人　弁理士　谷　義一　（外１名）

(54)【発明の名称】　センシティブ情報を相対的に安全度の低い記憶媒体に安全にストアする方法および装置

(57)【要約】

【課題】　相対的に安全度の高い記憶媒体と相対的に安全度の低い記憶媒体を含んでいるコンピュータ・システムにおいてセンシティブ情報を安全にストアする方法および装置が開示されている。

【解決手段】　センシティブ情報は暗号キーを使用して暗号化される。次に、暗号化されたセンシティブ情報は相対的に安全度の低い記憶媒体にストアされ、暗号キーは相対的に安全度の高い記憶媒体にストアされる。また、この装置によれば、暗号キー（３０２）がストアされる相対的に安全度の高い記憶媒体（２０８）と、相対的に安全度の低い記憶媒体（１０８，１０４）とを含んでいるコンピュータ・システムにおいて、センシティブ情報を安全にストアする。暗号化器（２０２）は暗号キーを使用してセンシティブ情報を暗号化し、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアする。



1

【特許請求の範囲】

【請求項１】　相対的に安全度の高い記憶媒体と相対的に安全度の低い記憶媒体とを備えたコンピュータ・システムにおいて、センシティブ情報を相対的に安全度の低い記憶媒体にストアする方法であって、
暗号キーを使用してセンシティブ情報を暗号化するステップと、
暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアするステップと、
暗号キーを相対的に安全度の高い記憶媒体にストアするステップとを含むことを特徴とする方法。

【請求項２】　請求項１に記載の方法において、
相対的に安全度の高い記憶媒体はプロセッサとメモリを含んでおり、さらに、
暗号キーをストアするステップは、
暗号キーをプロセッサに与えるステップと、
暗号キーをプロセッサからメモリに転送するステップとを含み、
センシティブ情報を暗号化するステップは、
センシティブ情報をプロセッサに与えるステップと、
プロセッサ内のセンシティブ情報を、以前にメモリにストアされた暗号キーを使用して暗号化するステップと、
相対的に安全度の低い記憶媒体にストアするために、暗号化されたセンシティブ情報をプロセッサから返却するステップとを含むことを特徴とする方法。

【請求項３】　請求項１に記載の方法において、
暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出すステップと、
取り出された暗号化されたセンシティブ情報を暗号キーを使用して暗号解読するステップとをさらに含むことを特徴とする方法。

【請求項４】　請求項１に記載の方法において、
相対的に安全度の高い記憶媒体はプロセッサとメモリを含んでおり、さらに、
センシティブ情報を暗号解読するステップは、
取り出された暗号化されたセンシティブ情報をプロセッサに与えるステップと、
プロセッサ内の取り出されたセンシティブ情報を暗号キーを使用して暗号解読するステップと、
暗号解読されたセンシティブ情報をプロセッサから返却するステップとを含むことを特徴とする方法。

【請求項５】　請求項３に記載の方法において、
センシティブ情報を暗号化するステップは暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップを含み、
暗号化されたセンシティブ情報をストアするステップは暗号チェックサムをストアするステップを含み、
暗号解読するステップは、
以前にストアされた暗号チェックサムを取り出すステップと、

2

ストアされた暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップと、
以前にストアされた暗号チェックサムを、新たに計算された暗号チェックサムと比較するステップと、
以前にストアされた暗号チェックサムが新たに計算された暗号チェックサムと不一致であれば、エラーを返却するステップとを含むことを特徴とする方法。

【請求項６】　請求項３に記載の方法において、
取り出すステップの前に、
取出し権限をユーザに要求するステップと、
取出し権限をユーザから受け取ったときだけ、取出しステップと暗号解読ステップを実行するステップとをさらに含むことを特徴とする方法。

【請求項７】　請求項６に記載の方法において、
取出し権限を要求するステップは、
識別ストリング(string)をユーザに要求するステップと、
ユーザから識別ストリングを受け取るステップと、
受け取った識別ストリングを、あらかじめ決めた識別ストリングと比較するステップと、
受け取った識別ストリングがあらかじめ決めた識別ストリングと一致していれば、取出し権限がユーザから受け取られたと判定するステップとを含むことを特徴とする方法。

【請求項８】　請求項７に記載の方法において、
暗号キーをストアするステップはあらかじめ決めた識別ストリングを相対的に安全度の高い記憶媒体にストアするステップを含むことを特徴とする方法。

【請求項９】　請求項７に記載の方法において、
暗号キーをストアするステップは、
あらかじめ決めた識別ストリングを暗号キーを使用して暗号化するステップと、
暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体にストアするステップとを含み、
比較するステップは、
暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体から取り出すステップと、
暗号化されたあらかじめ決めた識別ストリングを暗号ストリングを使用して暗号解読するステップと、
ユーザからの識別ストリングを、暗号解読されたあらかじめ決めた識別ストリングと比較するステップとを含むことを特徴とする方法。

【請求項１０】　請求項９に記載の方法において、
あらかじめ決めた識別ストリングを暗号化するステップはあらかじめ決めた識別ストリング全体にわたって暗号チェックサムを計算するステップを含み、
暗号化されたあらかじめ決めた識別ストリングをストアするステップは暗号チェックサムも相対的に安全度の低い記憶媒体にストアするステップを含み、

3

暗号化されたあらかじめ決めた識別ストリングを取り出すステップは以前にストアされた暗号チェックサムも取り出すステップを含み、
暗号化されたあらかじめ決めた識別ストリングを暗号解読するステップは、
あらかじめ決めた識別ストリング全体にわたって暗号チェックサムを計算するステップと、
計算された暗号チェックサムを、取り出された暗号チェックサムと比較するステップと、
計算された暗号チェックサムが取り出された暗号チェックサムと一致しているときだけ、受け取った識別ストリングを、暗号解読したあらかじめ決めた識別ストリングと比較するステップを実行するステップとを含むことを特徴とする方法。

【請求項１１】　請求項１に記載の方法において、
センシティブ情報を暗号化するステップは暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップを含み、
暗号化されたセンシティブ情報をストアするステップは暗号チェックサムを暗号化されたセンシティブ情報と一緒にストアするステップを含むことを特徴とする方法。

【請求項１２】　インタラクティブ・テレビジョン・システムにおいてセンシティブ情報を安全にストアするプロセッサ装置であって、
暗号キーをストアするための相対的に安全度の高い記憶媒体と、
相対的に安全度の低い記憶媒体と、
相対的に安全度の低い記憶媒体に結合されていて、暗号キーに応答してセンシティブ情報を暗号化し、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアする暗号化器とを備えていることを特徴とする装置。

【請求項１３】　請求項１２に記載の装置において、
暗号解読器をさらに含み、該暗号解読器は相対的に安全度の低い記憶媒体に結合されていて、暗号キーに応答して暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出し、暗号化されたセンシティブ情報を暗号解読することを特徴とする装置。

【請求項１４】　請求項１３に記載の装置において、
暗号解読器は取出し権限をユーザに要求し、取出し権限をユーザから受け取ったときだけ、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出し、暗号化されたセンシティブ情報を暗号解読する回路を含むことを特徴とする装置。

【請求項１５】　請求項１４に記載の装置において、
取出し権限を要求する回路は、
識別ストリングをユーザに要求する回路と、
受け取った識別ストリングをあらかじめ決めた識別ストリングと比較し、受け取った識別ストリングがあらかじめ決めた識別ストリングと一致していれば、取出し権限

4

が受け取られたと判定する回路とを含むことを特徴とする装置。

【請求項１６】　請求項１５に記載の装置において、
あらかじめ決めた識別ストリングは暗号化された形態で相対的に安全度の低い記憶媒体にストアされ、暗号解読器は、さらに、
暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体から受け取る回路と、
前記受け取った暗号化されたあらかじめ決めた識別ストリングを暗号解読する回路とを含むことを特徴とする装置。

【請求項１７】　請求項１２に記載の装置において、
相対的に安全度の高い記憶媒体は、
マイクロプロセッサと、
システム・バスを介してマイクロプロセッサに結合されていて、暗号キーをストアするためのメモリとを含んでおり、
暗号化器と暗号解読器はマイクロプロセッサに含まれていることを特徴とする装置。

【請求項１８】　請求項１７に記載の装置において、
相対的に安全度の低い記憶媒体は、
別のマイクロプロセッサと、
システム・バスを介してマイクロプロセッサに結合されていて、暗号化されたセンシティブ情報をストアするための読み書きメモリとを含んでいることを特徴とする装置。

【請求項１９】　請求項１８に記載の装置において、
相対的に安全度の高い記憶媒体はさらに入出力ポートを含み、該入出力ポートは相対的に安定度の高い記憶媒体側のシステム・バスを介して、相対的に安定度の高い記憶媒体側のマイクロプロセッサとメモリに結合されており、
相対的に安定度の低い記憶媒体はさらに入出力ポートを含み、該入出力ポートは相対的に安定度の低い記憶媒体側のシステム・バスを介して、相対的に安定度の低い記憶媒体側の別のマイクロプロセッサとメモリに結合されており、
相対的に安定度の高い記憶媒体側の入出力ポートは相対的に安定度の低い記憶媒体側の入出力ポートに結合されていることを特徴とする装置。

【請求項２０】　請求項１２に記載の装置において、
さらに、前記暗号化されたセンシティブ情報全体にわたってチェックサムを生成し、当該チェックサムを、ストアされた前記暗号化されたセンシティブ情報に付加する回路と、
ストアされた前記暗号化されたセンシティブ情報全体にわたって別のチェックサムを生成し、当該別のチェックサムを、前記ストアされた暗号化されたセンシティブ情報に付加された前記チェックサムと比較する回路と、
前記チェックサムと前記別のチェックサムが同一である

5

ことを条件として、前記ストアされた暗号化されたセンシティブ情報を暗号解読する暗号解読器とを含むことを特徴とする装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、センシティブ情報を相対的に安全度の低い記憶媒体にストアする方法および装置に関する。

【０００２】なお、本明細書の記述は本件出願の優先権の基礎たる米国特許出願第０８／４９９，１７０号（１９９５年７月７日出願）の明細書の記載に基づくものであって、当該米国特許出願の番号を参照することによって当該米国特許出願の明細書の記載内容が本明細書の一部分を構成するものとする。

【０００３】

【従来の技術】センシティブ情報（例えば、クレジットカード番号または暗号キー）をコンピュータ・システムにストアしておく必要がしばしば起こっている。しかし、かかるセンシティブ情報のストアの仕方が安全でないと、その情報が変更されたり、盗まれたりする可能性がある。コンピュータ・システムへのアクセスを信用のある人だけに制限し、信用のあるプログラムだけをコンピュータ・システムで実行することは、この問題を解決する1つの方法である。しかし、この解決方法は常に実用的であるとは限らない。第三者による使用を目的としていても、第三者によるアクセスを認めなければ、無用になってしまうコンピュータ・システムが存在するからである。例えば、インタラクティブ（対話型）テレビジョン・システムのようなマルチメディア・システムでは、ユーザのデコーダはユーザのセンシティブ情報をストアしているが、見知らぬ第三者が書いたプログラムを実行するために、やむを得ずそのデコーダが利用されることがある。

【０００４】インタラクティブ・テレビジョン・アプリケーションはビデオ（映像）部分、オーディオ（音声）部分およびコンピュータ・プログラム部分からなっている。このインタラクティブ・テレビジョン・アプリケーションは、中央のブロードキャスト・ロケーションから遠隔地の視聴者(viewer)ロケーションへコンポジット信号でブロードキャスト（同報通信）されている。各視聴者のロケーションにはレシーバ／デコーダが置かれており、これらはインタラクティブ・テレビジョン・アプリケーションのコンポジット信号を検出・出力し、ビデオ部分、オーディオ部分およびコンピュータ・プログラム部分を分離し、テレビジョン・レシーバが必要とするビデオ信号とオーディオ信号を生成し、コンピュータ・プログラムを実行して視聴者と対話している。各デコーダは電話インタフェースも備えているので、コンピュータ・プログラムの制御の下で（およびユーザの許可を得て）データ・コール（起呼）を行って、リモート・ロケーションとの間で情報（実行すべきコンピュータ・プログラム・コードを含む）を送受信することを可能にしている。

6

【０００５】

【発明が解決しようとする課題】ここで検討しようとしている１つのインタラクティブ・アプリケーションはショッピング・アプリケーションであり、このアプリケーションでは、以前にデコーダに入力されていた視聴者のクレジットカード番号は、視聴者がオーダを出したとき、安全な方法で（ユーザの許可を得て）ショッピング・プログラム提供者へ送られるようにしている。そのために、視聴者のクレジットカード番号はデコーダにストアしておく必要がある。しかし、コンピュータ・プログラムはブロードキャストまたは電話リンクを通してロード可能であるので、そのコンピュータ・プログラムが視聴者のクレジットカード番号や他のセンシティブ情報を盗んでそれを、例えば、電話リンクを通して第三者へ中継しようとすることも起こり得る。

【０００６】センシティブ情報を安全に維持するための１つの方法では、コンピュータ・システムの公用部分と、センシティブ情報がストアされる部分との間の障壁となるために、ハードウェアをコンピュータ・システムに接続することが要件になっている。しかし、ハードウェアによる解決は高価である。これは、コンシューマ・プロダクトであるインタラクティブ・テレビジョン・システムでは、コストに非常に敏感であるために特に問題である。そのために、この種のシステムで利用可能にされる安全保護ハードウェア量は、最小限の情報を収容して、保護するような設計になっている。しかし、盗難から保護する必要のあるセンシティブ情報は大量化する潜在性をもっている。望ましいことは、比較的に大量のセンシティブ情報を変更または盗難から保護し、しかも、高価な安全保護ハードウェアを大量に使用しないで済むようにすることである。

【０００７】

【課題を解決するための手段】本発明の原理によれば、相対的に安全度の高い記憶媒体と相対的に安全度の低い記憶媒体を備えたコンピュータ・システムにおいて、センシティブ情報を安全にストアする方法は次のようなステップからなっている。センシティブ情報は暗号キーを使用して暗号化される。暗号化されたセンシティブ情報は相対的に安全度の低い記憶媒体にストアされ、暗号キーは相対的に安全度の高い記憶媒体にストアされる。

【０００８】コンピュータ・システムにおいてセンシティブ情報を安全にストアする装置は暗号キーがストアされる相対的に安全度の高い記憶媒体と、相対的に安全度の低い記憶媒体とを含んでいる。暗号化器 (encrypter) は暗号キーを使用してセンシティブ情報を暗号化し、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアする。

7

【０００９】請求項１にかかる発明は、相対的に安全度の高い記憶媒体と相対的に安全度の低い記憶媒体とを備えたコンピュータ・システムにおいて、センシティブ情報を相対的に安全度の低い記憶媒体にストアする方法であって、暗号キーを使用してセンシティブ情報を暗号化するステップと、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアするステップと、暗号キーを相対的に安全度の高い記憶媒体にストアするステップとを含むことを特徴とする。

【００１０】また、請求項２にかかる発明は、請求項１に記載の方法において、相対的に安全度の高い記憶媒体はプロセッサとメモリを含んでおり、さらに、暗号キーをストアするステップは、暗号キーをプロセッサに与えるステップと、暗号キーをプロセッサからメモリに転送するステップとを含み、センシティブ情報を暗号化するステップは、センシティブ情報をプロセッサに与えるステップと、プロセッサ内のセンシティブ情報を、以前にメモリにストアされた暗号キーを使用して暗号化するステップと、相対的に安全度の低い記憶媒体にストアするために、暗号化されたセンシティブ情報をプロセッサから返却するステップとを含むことを特徴とする。

【００１１】さらに、請求項３にかかる発明は、請求項１に記載の方法において、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出すステップと、取り出された暗号化されたセンシティブ情報を暗号キーを使用して暗号解読するステップとをさらに含むことを特徴とする。

【００１２】さらに、請求項４にかかる発明は、請求項１に記載の方法において、相対的に安全度の高い記憶媒体はプロセッサとメモリを含んでおり、さらに、センシティブ情報を暗号解読するステップは、取り出された暗号化されたセンシティブ情報をプロセッサに与えるステップと、プロセッサ内の取り出されたセンシティブ情報を暗号キーを使用して暗号解読するステップと、暗号解読されたセンシティブ情報をプロセッサから返却するステップとを含むことを特徴とする。

【００１３】さらに、請求項５にかかる発明は、請求項３に記載の方法において、センシティブ情報を暗号化するステップは暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップを含み、暗号化されたセンシティブ情報をストアするステップは暗号チェックサムをストアするステップを含み、暗号解読するステップは、以前にストアされた暗号チェックサムを取り出すステップと、ストアされた暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップと、以前にストアされた暗号チェックサムを、新たに計算された暗号チェックサムと比較するステップと、以前にストアされた暗号チェックサムが新たに計算された暗号チェックサムと不一致であれば、エラーを返却するステップとを含むことを特徴とする。

8

【００１４】さらに、請求項６にかかる発明は、請求項３に記載の方法において、取り出すステップの前に、取出し権限をユーザに要求するステップと、取出し権限をユーザから受け取ったときだけ、取出しステップと暗号解読ステップを実行するステップとをさらに含むことを特徴とする。

【００１５】さらに、請求項７にかかる発明は、請求項６に記載の方法において、取出し権限を要求するステップは、識別ストリング(string)をユーザに要求するステップと、ユーザから識別ストリングを受け取るステップと、受け取った識別ストリングを、あらかじめ決めた識別ストリングと比較するステップと、受け取った識別ストリングがあらかじめ決めた識別ストリングと一致していれば、取出し権限がユーザから受け取られたと判定するステップとを含むことを特徴とする。

【００１６】さらに、請求項８にかかる発明は、請求項７に記載の方法において、暗号キーをストアするステップはあらかじめ決めた識別ストリングを相対的に安全度の高い記憶媒体にストアするステップを含むことを特徴とする。

【００１７】さらに、請求項９にかかる発明は、請求項７に記載の方法において、暗号キーをストアするステップは、あらかじめ決めた識別ストリングを暗号キーを使用して暗号化するステップと、暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体にストアするステップとを含み、比較するステップは、暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体から取り出すステップと、暗号化されたあらかじめ決めた識別ストリングを暗号ストリングを使用して暗号解読するステップと、ユーザからの識別ストリングを、暗号解読されたあらかじめ決めた識別ストリングと比較するステップとを含むことを特徴とする方法。

【００１８】さらに、請求項１０にかかる発明は、請求項９に記載の方法において、あらかじめ決めた識別ストリングを暗号化するステップはあらかじめ決めた識別ストリング全体にわたって暗号チェックサムを計算するステップを含み、暗号化されたあらかじめ決めた識別ストリングをストアするステップは暗号チェックサムも相対的に安全度の低い記憶媒体にストアするステップを含み、暗号化されたあらかじめ決めた識別ストリングを取り出すステップは以前にストアされた暗号チェックサムも取り出すステップを含み、暗号化されたあらかじめ決めた識別ストリングを暗号解読するステップは、あらかじめ決めた識別ストリング全体にわたって暗号チェックサムを計算するステップと、計算された暗号チェックサムを、取り出された暗号チェックサムと比較するステップと、計算された暗号チェックサムが取り出された暗号チェックサムと一致しているときだけ、受け取った識別ストリングを、暗号解読したあらかじめ決めた識別スト

9

リングと比較するステップを実行するステップとを含むことを特徴とする。

【００１９】さらに、請求項１１にかかる発明は、請求項１に記載の方法において、センシティブ情報を暗号化するステップは暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップを含み、暗号化されたセンシティブ情報をストアするステップは暗号チェックサムを暗号化されたセンシティブ情報と一緒にストアするステップを含むことを特徴とする。

【００２０】さらに、請求項１２にかかる発明は、インタラクティブ・テレビジョン・システムにおいてセンシティブ情報を安全にストアするプロセッサ装置であって、暗号キーをストアするための相対的に安全度の高い記憶媒体（２０８）と、相対的に安全度の低い記憶媒体（１０８，１０４）と、相対的に安全度の低い記憶媒体に結合されていて、暗号キー（３０２）に応答してセンシティブ情報を暗号化し、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアする暗号化器（２０２）とを備えていることを特徴とする。

【００２１】さらに、請求項１３にかかる発明は、請求項１２に記載の装置において、暗号解読器をさらに含み、該暗号解読器は相対的に安全度の低い記憶媒体に結合されていて、暗号キーに応答して暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出し、暗号化されたセンシティブ情報を暗号解読することを特徴とする。

【００２２】さらに、請求項１４にかかる発明は、請求項１３に記載の装置において、暗号解読器は取出し権限をユーザに要求し、取出し権限をユーザから受け取ったときだけ、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出し、暗号化されたセンシティブ情報を暗号解読する回路を含むことを特徴とする。

【００２３】さらに、請求項１５にかかる発明は、請求項１４に記載の装置において、取出し権限を要求する回路は、識別ストリングをユーザに要求する回路と、受け取った識別ストリングをあらかじめ決めた識別ストリングと比較し、受け取った識別ストリングがあらかじめ決めた識別ストリングと一致していれば、取出し権限が受け取られたと判定する回路とを含むことを特徴とする。

【００２４】さらに、請求項１６にかかる発明は、請求項１５に記載の装置において、あらかじめ決めた識別ストリングは暗号化された形態で相対的に安全度の低い記憶媒体にストアされ、暗号解読器は、さらに、暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体から受け取る回路と、前記受け取った暗号化されたあらかじめ決めた識別ストリングを暗号解読する回路とを含むことを特徴とする。

【００２５】さらに、請求項１７にかかる発明は、請求項１２に記載の装置において、相対的に安全度の高い記

10

憶媒体は、マイクロプロセッサと、システム・バスを介してマイクロプロセッサに結合されていて、暗号キーをストアするためのメモリとを含んでおり、暗号化器と暗号解読器はマイクロプロセッサに含まれていることを特徴とする。

【００２６】さらに、請求項１８にかかる発明は、請求項１７に記載の装置において、相対的に安全度の低い記憶媒体は、別のマイクロプロセッサと、システム・バスを介してマイクロプロセッサに結合されていて、暗号化されたセンシティブ情報をストアするための読み書きメモリとを含んでいることを特徴とする。

【００２７】さらに、請求項１９にかかる発明は、請求項１８に記載の装置において、相対的に安全度の高い記憶媒体はさらに入出力ポートを含み、該入出力ポートは相対的に安定度の高い記憶媒体側のシステム・バスを介して、相対的に安定度の高い記憶媒体側のマイクロプロセッサとメモリに結合されており、相対的に安定度の低い記憶媒体はさらに入出力ポートを含み、該入出力ポートは相対的に安定度の低い記憶媒体側のシステム・バスを介して、相対的に安定度の低い記憶媒体側の別のマイクロプロセッサとメモリに結合されており、相対的に安定度の高い記憶媒体側の入出力ポートは相対的に安定度の低い記憶媒体側の入出力ポートに結合されていることを特徴とする。

【００２８】さらに、請求項２０にかかる発明は、請求項１２に記載の装置において、さらに、前記暗号化されたセンシティブ情報全体にわたってチェックサムを生成し、当該チェックサムを、ストアされた前記暗号化されたセンシティブ情報に付加する回路と、ストアされた前記暗号化されたセンシティブ情報全体にわたって別のチェックサムを生成し、当該別のチェックサムを、前記ストアされた暗号化されたセンシティブ情報に付加された前記チェックサムと比較する回路と、前記チェックサムと前記別のチェックサムが同一であることを条件として、前記ストアされた暗号化されたセンシティブ情報を暗号解読する暗号解読器とを含むことを特徴とする。

【００２９】

【発明の実施の形態】図１は、本発明を取り入れているイタラクティブ・テレビジョン・デコーダを示すブロック図である。図１に示すように、セット・トップ・ボックス(set topbox) １０はスマート・カード２０に結合されている。スマート・カード２０は例えば、クレジットカードとほぼ同サイズの小型デバイスであり、これはセット・トップ・ボックス１０内のコネクタ３０に挿入される。セット・トップ・ボックス１０はＣＰＵ１０２を内蔵しており、このＣＰＵは、システム・バス１１０を介して公知のようにＲＡＭ１０４、ＲＯＭ１０６、ＥＥＰＲＯＭ１０８および入出力（Ｉ／Ｏ）ポート１１２に結合されている。セット・トップ・ボックス１０は他の入出力ポート（図示せず）も備えており、これらもシ

11

ステム・バス１１０に結合されている。これらの入出力ポートは、例えば、ブロードキャスト・インタラクティブ・テレビジョン・コンポジット信号を受信し、テレビジョン・モニタおよびスピーカ用のビデオ信号とオーディオ信号を出力し、電話システム経由でリモート・コンピュータに接続し、および／または視聴者ロケーションに置かれたローカル・パーソナル・コンピュータに接続するためのものである。入出力アダプタをどのように設計し製造すると、これらのサービスが得られるか、また、これらのアダプタをどのようにシステム・バス１１０に接続するかは、コンピュータ・システム設計分野に精通したものならば当然に理解されることである。

【００３０】スマート・カード２０はＣＰＵ２０２を内蔵し、このＣＰＵは、システム・バス２１０を介して公知のようにＲＡＭ２０４、ＲＯＭ２０６、ＥＥＰＲＯＭ２０８および入出力ポート２１２に結合されている。セット・トップ・ボックス１０側の入出力ポート１１２は、コネクタ３０を介してスマート・カード２０側の入出力ポート２１２に結合されている。

【００３１】図２は一部がブロック図に、一部がデータフロー図になっているが、これは、図１に示すセット・トップ・ボックス１０とスマート・カード２０のオペレーションの理解を容易にするためである。図２に示すエレメントで、図１に示されているものには、同一の参照符号を付けてあり、以下で詳しく説明することは省略する。図２に示すラインは図示エレメント間のデータの流れを示すもので、それぞれの物理的接続を示したものではない。

【００３２】図１を参照してオペレーションを説明すると、セット・トップ・ボックス１０内のＣＰＵ１０２はＲＡＭ１０４、ＥＥＰＲＯＭ１０８、および入出力ポート１１２などの入力ポートからデータを取り出し、そのデータを処理し、処理したデータをＲＡＭ１０４やＥＥＰＲＯＭ１０８にストアしておくことも、処理したデータを入出力ポート１１２などの出力ポートへ渡すこともできるが、これらはすべて、ＲＯＭ１０６に格納されているプログラムの制御を受けて公知の方法で行われる。図２に示すように、ＥＥＰＲＯＭ１０８は、システムに関する情報４２０を収めているシステム部分４１６と、ユーザに関する情報４２２を収めているユーザ部分４１８を含むように区画化されている。同様に、ＲＡＭ１０４も、システムに関する情報を収めているシステム部分４２４と、ユーザに関する情報を収めているユーザ部分４２６を含むように区画化されている。

【００３３】ブロードキャストまたは電話リンク（図示せず）を介してセット・トップ・ボックス１０に渡されるインタラクティブ・プログラムはトークンの形体になっており、これは、公知のように、セット・トップ・ボックス１０内のインタプリタによって解釈される。インタラクティブ・プログラムは１つまたは２つ以上のコード・モジュールと、場合によっては、１つまたは２つ以上のデータ・モジュールとからなっている。図４に示すように、コード・モジュールはＲＡＭ１０４内のコード・セクション４０２に格納され、データ・モジュールはデータ・セクション４０４に格納されている。ＲＯＭ１０６に格納されているインタプリタ４０６はセット・トップ・ボックス１０内のＣＰＵ１０２によって実行され、それぞれがＲＡＭ１０４のコード・セクション４０２とデータ・セクション４０４に置かれているコード・モジュールとデータ・モジュールを解釈するように動作する。インタラクティブ・プログラムは、インタプリタ4,06の制御の下でデータをデータ部分４０４から読み取り、そのデータを処理し、変更したデータをデータ部分４０４に書き戻すことができる。また、インタプリタ４０６は、同じくＲＯＭ１０６に格納されているハードウェア・ドライバ４０８へのプログラム・コールを通して、公知のようにセット・トップ・ボックス１０内のハードウェアともやりとりする。

12

【００３４】ライブラリ・ルーチン群４１０は、インタプリタ４０６からプログラム・コールを通してアクセス可能であるが、共通に必要になるファンクション（functions）用に用意されたものである。スマート・カード入出力ドライバ４０８Ａ、ＥＥＰＲＯＭ１０８、およびＲＡＭ１０４，４２４および４２６のシステム部分とユーザ部分がアクセスできるのは、ライブラリ・ルーチン４１０への正しいコールを通してだけである。ライブラリ・ルーチン４１０はユーザの許可を要求し、それを受け取ってからセンシティブ情報を上記ソースのいずれかからインタラクティブ・システムへ返却するように事前にプログラムしておくことが可能である。基本的には、ライブラリ・ルーチン４１０は、それぞれＥＥＰＲＯＭ１０８およびＲＡＭ１０４，４２４，４２６のシステム部分とユーザ部分に格納されているデータのソフトウェア・ゲートキーパ（門番）の働きをする。ライブラリ・ルーチン４１０にゲートキーパ機能があるために、ＥＥＰＲＯＭ１０８およびＲＡＭ１０４，４２４，４２６のシステム部分とユーザ部分は、それぞれＲＡＭ１０４，４０２，４０４のコード部分とデータ部分よりも相対的に安全度の高い記憶媒体になっている。さらに、ＥＥＰＲＯＭ１０８はＲＡＭ１０４から物理的に切り離されているので、ＥＥＰＲＯＭ１０８はＲＡＭ１０４よりも相対的に安全度の高い記憶媒体になっている。

【００３５】図１に戻って説明すると、スマート・カード２０内のＣＰＵ２０２は、入出力ポート２１２経由でセット・トップ・ボックス１０からデータを受け取り、その情報を処理し、入出力ポート２１２経由で情報をセット・トップ・ボックス１０へ返却するようにプログラムされており、これらはすべてＲＯＭ２０４に格納されたプログラムの制御の下で行われる。ＲＯＭ２０４に事前プログラムされているオペレーションだけが、スマー

13

ト・カード２０内のＣＰＵ２０２によって実行される。例えば、セット・トップ・ボックス１０の購入時に、購入者をユニークに識別すると共に、暗号解読（および暗号）キーの働きをするマスタ・キーは、入力ポート２１２からスマート・カード２０に入力される。マスタ・キーは非常にセンシティブな情報である。スマート・カード２０内のＣＰＵ２０２はマスタ・キーをＥＥＰＲＯＭ２０８にストアするようにプログラムされている。図２に示すように、スマート・カード２０内のＥＥＰＲＯＭ２０８はシステム部分とユーザ部分に分割することが可能である。ＣＰＵ２０２はマスタ・キー３０２をＥＥＰＲＯＭ２０８のシステム部分にストアする。

【００３６】図１に戻って説明すると、暗号化されたデータがブロードキャストからセット・トップ・ボックス１０によって受信され、暗号解読する必要があるときは、その暗号化データは入出力ポート２１２からスマート・カード２０に渡される。スマート・カード２０内のＣＰＵ２０２はＥＥＰＲＯＭ２０８に以前にストアされていたマスタ・キー３０２を使用して、暗号化データを暗号解読し、プレーンテキスト（plaintext）を入出力ポート２１２経由でセット・トップ・ボックス１０へ返却する。同様に、ＣＰＵ２０２は入出力ポート２１２から受け取ったプレーンテキストを暗号化し、暗号化されたデータを入出力ポート２１２経由でセット・トップ・ボックス１０へ送り返す。ＣＰＵ２０２はマスタ・キー３０２をセット・トップ・ボックス１０へ戻すようにプログラムされていないので、セット・トップ・ボックス１０で実行されているプログラムがマスタ・キー３０２を変更したり、取得したりすること、場合によっては、マスタ・キーを盗むことは不可能である。ＣＰＵ２０２はスマート・カード２０に格納されたデータのハードウェア・ゲートキーパ（門番）の働きをするので、セット・トップ・ボックス１０側のＥＥＰＲＯＭ１０８またはＲＡＭ１０４よりも相対的に安全度が高く、非常に安全度の高い記憶媒体になっている。

【００３７】上述したように、セット・トップ・ボックス１０側のＥＥＰＲＯＭ１０８とＲＡＭ１０４はスマート・カード２０側のＣＰＵ２０２のようなハードウェア・ゲートキーパによって保護されていない。その代わりに、ＥＥＰＲＯＭ１０８とＲＡＭ１０４の保護はライブラリ・ルーチン４１０を通してソフトウェアで実現されている。しかし、ＥＥＰＲＯＭ１０８とＲＡＭ１０４はソフトウェアによって保護されるので、その保護が偶然にしろ、意図的にしろ、他のソフトウェアによって違反される可能性が常にある。インタラクティブ・プログラムは、保護ソフトウェアをだますことによってＥＥＰＲＯＭ１０８またはＲＡＭ１０４へアクセスできる潜在性をもっている。例えば、正しくないデータがリロケーション（再配置）プロセス期間にプログラム・ローダ（図示せず）に渡されたり、あるいはプログラム・スタック

14

（図示せず）がプログラム実行中に意図的にオーバフローしたりするおそれがある。要するに、ソフトウェア保護が他のプログラムによって破られるおそれがある。

【００３８】上述したように、最も安全度が高い記憶媒体はスマート・カード２０であり、次に安全度が高いのはセット・トップ・ボックス１０内のＥＥＰＲＯＭ１０８であり、次がＲＡＭ１０４のシステム部分４１２とユーザ部分４１４であり、最も安全度が低いのがＲＡＭ１０４のコード部分４０２とデータ部分４０４である。センシティブ情報のセキュリティ（安全保護）を最大にするには、この情報は、マスタ・キー３０２と同じように、スマート・カード２０側のＥＥＰＲＯＭ２０８に置いておくべきである。しかし、スマート・カード２０側のＥＥＰＲＯＭ２０８のサイズは限られているので、センシティブ情報をストアできるスペースはわずかしか残っていない場合がある（マスタ・キー３０２は別として）。あるいは、スペースがまったく残っていない場合も起こり得る。セット・トップ・ボックス１０側のＥＥＰＲＯＭ１０８のサイズも、同様に限られているので、センシティブ情報をストアできるスペースはわずかしか残っていない場合もあれば、まったく残っていない場合もある。従って、ユーザのセンシティブ情報の大部分はＲＡＭ１０４にストアせざる得ないことになるが、これは最も安全度の低い記憶媒体である。

【００３９】スマート・カード２０にストアできる以上のセンシティブ情報量を安全にストアするために、まず、センシティブ情報は上述したように、スマート・カード20にストアされたマスタ・キー３０２を使用してスマート・カード２０側のＣＰＵ２０２によって暗号化される（例えば、データ暗号化規格（Data Encryption Standard - ＤＥＳ）を使用して）。そのあと、暗号化されたセンシティブ情報は相対的に安全度の低いＥＥＰＲＯＭ１０８にストアすることも、ＲＡＭ１０４のシステム部分４１２またはデータ部分４１４にストアすることも可能である。さらに、センシティブ情報の変更を防止するために、センシティブ情報全体にわたる暗号チェックサムも、例えば、市販されているハッシュ関数 MD5などの、一方向暗号ハッシュ関数（one-way cryptographic hash function）を使用して計算され、情報に付加される。（ＭＤ５はCounterpane Systems 社、730 Fair Oaks Ave., Oak Park Illinois, 60302からディスケットに入って提供されている。）チェックサムはプレーンテキストのセンシティブ情報全体にわたって生成することも、暗号化されたセンシティブ情報全体にわたって生成することも、その両方で生成することも可能である。好適実施例では、チェックサムは暗号化されたセンシティブ情報全体にわたって生成されている。チェックサムは、ＣＰＵ２０２またはＣＰＵ１０２を使用してソフトウェアで生成することも、バス構造に結合された専用ハードウェア・ハッシュ関数エレメント（図示せず）で生

15

成することも可能である。暗号化されたセンシティブ情報をアクセスできないプログラムは、スマート・カード２０に格納されているマスタ・キー３０２がなければ、その情報を暗号解読して、読み取ることはできない。さらに、暗号化された情報を変更しようとしても、その試みは、以前に計算されて情報に付加された暗号チェックサムと、新たに取り出したセンシティブ情報全体にわたって同じように計算された暗号チェックサムとの不一致によって検出される。

【００４０】スマート・カード２０はデータを暗号化する前に、ユーザの許可を要求する。これは、パーソナル識別番号（ＰＩＮ）をユーザに要求することにより行われる。なお、このＰＩＮは好ましくは４～６文字のＩＤになっている。ＰＩＮはセット・トップ・ボックス１０のベンダに選択させ、あとでユーザが変更することができる。ユーザが与えたＰＩＮが現在格納されているＰＩＮに一致していれば、データは暗号解読される。正しくないＰＩＮがあらかじめ決めた回数（例えば、４回）続けて入力されると、ユーザ以外のだれかがセット・トップ・ボックス１０に侵入しようとしているものとみなされるので、マスタ・キー３０２は使用禁止にされる。

【００４１】図２に示すように、セキュリティを最大にするために、ＰＩＮ３０４はスマート・カード２０にストアされる。ＰＩＮ３０４はわずか４～６文字であり、４～６バイトにストアできるため、スマート・カード２０側のＥＥＰＲＯＭ２０８にはＰＩＮ３０４をストアするだけの空きスペースを残すことができる。スマート・カード２０側のＣＰＵ２０２がＰＩＮ３０４をリリースしないようにプログラムされていれば、ＰＩＮ３０４をより安全に格納しておくことができる。視聴者が正しいＰＩＮ３０４を与えたときだけ、スマート・カード２０は、要求側プログラムのためにセンシティブ・データを暗号解読する。これにより、センシティブ・データのリリースは安全な状態で視聴者の制御下に置かれることになる。

【００４２】二次暗号キー、クレジットカード番号などのように、電源障害が起こったときユーザが残しておきたいと思っているセンシティブ情報は、セット・トップ・ボックス１０側のＥＥＰＲＯＭ１０８にストアされる。この情報はスマート・カード２０に入っているマスタ・カード３０２を使用して暗号化される。暗号化されたセンシティブ・システム情報４２０はセット・トップ・ボックス１０側のＥＥＰＲＯＭ１０８のシステム部分４１６にストアされ、暗号化されたセンシティブ・ユーザ情報４２２はＥＥＰＲＯＭ１０８のユーザ部分４１８にストアされる。暗号化されたセンシティブ・システム情報４２０またはユーザ情報４２２をアクセスしようとする不正プログラムはその暗号解読をスマート・カード２０に要求しなければならないので、ユーザから正しいＰＩＮを受け取らない限り、スマート・カード２０はその要求を拒否することになる。ＰＩＮをランダムに送ってスマート・カードに侵入しようとすると、その試みが数回失敗したあとでマスタ・キー３０２は使用禁止にされる。

16

【００４３】しかし、上述したように、ＥＥＰＲＯＭ１０８も、センシティブ情報をストアできるスペースが限られている。従って、電源障害が起こったとき残しておきたい重要な情報だけが上記と同じようにＥＥＰＲＯＭ１０８にストアされる。図３に示すように、相対的に安定度の低いＲＡＭ１０４には、もっと多くのセンシティブ情報をストアすることが可能である。この情報は暗号化され、暗号チェックサムはＥＥＰＲＯＭ１０８のシステム部分４１６に暗号化形式で格納されている二次暗号キーの１つを使用して付加される。暗号化されたセンシティブ・システム情報はＲＡＭ１０４のシステム部分４１２にストアされ、暗号化されたセンシティブ・ユーザ情報はＲＡＭ１０４のユーザ部分４１４にストアされる。ＲＡＭ１０４のメモリ要求量は低下しているので、もっと多くのセンシティブ情報をＲＡＭ１０４にストアすることができる。

【００４４】この情報をアクセスするには、ＥＥＰＲＯＭ１０８に格納されている、暗号化された二次暗号キーがまず暗号解読されなければならない。二次暗号キー自体も、スマート・カード２０に格納されたマスタ・キー３０２を使用して以前に暗号化されているので、上述したように、この二次暗号キーがスマート・カード２０によって暗号解読されるのは、これも上述したように、ユーザの許可を受け取ったあとだけである。暗号解読された二次キーがスマート・カード２０から返されれば、ＲＡＭ１０４にストアされたセンシティブ情報はこのキーを使用して暗号解読することができる。ＲＡＭ１０４には、ＥＥＰＲＯＭ１０８やスマート・カード２０よりも多くのスペースが残っているので、より多くのセンシティブ情報をＲＡＭ１０４にストアすることができる。その場合でも、この情報が無断アクセスから保護されているのは、その暗号解読のためには、スマート・カード２０にストアされているマスタ・キーが最終的に必要になるためである。

【００４５】図４に示すように、上述した手法はユーザＰＩＮをストアするだけのスペースがスマート・カード２０に残っていない場合でも使用することができる。図４に示すように、マスタ・キー３０２だけがスマート・カード２０にストアされている。ＰＩＮは暗号化され、暗号チェックサムはマスタ・キー３０２を使用して付加され、暗号化されたＰＩＮ３０４′はシステム情報４２０の一部として、セット・トップ・ボックス１０側のＥＥＰＲＯＭ１０８のシステム部分４１６にストアされる。図４に示す実施例では、スマート・カード２０はデータを暗号解読するように要求されると、暗号化されたＰＩＮ３０４′をＥＥＰＲＯＭ１０８から取り出し、そ

17

れを暗号解読して、その暗号チェックサムを以前にストアされた暗号チェックサムと比較する。暗号チェックサムが同一であれば、ＰＩＮがユーザに要求され、暗号解読されたＰＩＮと比較される。これらが同一であれば、要求されたデータが暗号解読される。上述したように、正しくないＰＩＮ番号が続けて入力されると、マスタ・キー３０２のオペレーションは禁止される。また、上述したように、センシティブ情報は暗号化してＲＡＭ１０４にストアすることができる。

【００４６】セット・トップ・ボックス１０の特定実施例によれば、独自の公用－私用キーのペアが生成され、ストアされ、管理されるようになっている。このような実施例では、セット・トップ・ボックス、つまり、ＢＯＸは、シグネーチャ（署名）に対してRivest、ShamirおよびAdleman 公用キー・アルゴリズムＲＳＡを採用するように構成されている。ＲＳＡアルゴリズムでは、２つの基数ｐとｑ（ただし、ｐ＜ｑ）、およびサイズBOX PUBLIC MODULUS SIZE/2 とサイズBOX EXPONENT SIZE の任意の指数“ｅ”の各々を生成し、ストアすることが要件になっている。これらの３つの値ｐ，ｑ，ｅからは、ＲＳＡ暗号化を行うための、他のすべてのパラメータを求めるとき必要になる一切の情報が得られる。しかし、公用キーの各シグネーチャまたは照会ごとに他のパラメータを求めるために計算負担 (penalty) が伴うことは望ましくないので、システムはパラメータを一度だけ（または少なくともＢＯＸがリセットされるたびに）生成し、それぞれの値をストアしておいて、反復的に使用するようにしている。これらの値はＢＯＸ内の安全保護された不揮発性メモリにストアしておくべきであるが、この種の記憶容量は上述したように限られている。従って、これらの値はＲＡＭに安全にストアされて、データの保全性と機密性が保証されるようにしている。

【００４７】上述したことは次のように行われる。値ｐとｑは生成されるか、あるいは与えられて、ＢＯＸモジュラス (modulus) “ｎ”がｎ＝ｐ×ｑに従ってＢＯＸＣＰＵ１０２またはスマート・カードＣＰＵ２０２によって計算される。ＢＯＸ　ＥＸＰＯＮＥＮＴ値“ｅ”は選択されるか、あるいはあらかじめ決められて、ＥＥＰＲＯＭ１０８などの不揮発性ストレージ (storage) にストアされる。値ｎとｅは、アクセスを容易にするためにプレーンテキストとしてＲＡＭ１０４にストアされる。値ｎとｅは公用キーとなり、従って、公用キー・システムでは公衆に知らされるので、機密に保持しておく必要はない。値ｐとｑは、シード・ワード (seed word) が１２８ビットに初期設定されている疑似乱数ジェネレータを使用して生成される。この疑似乱数ジェネレータは、少なくともその一部にＭＤ５などのハッシュ関数を含めることができ、ＣＰＵによってソフトウェアで実行させることが可能である。

【００４８】その他の値（私用キーを得るための）はＣ

18

ＰＵによって次のように計算される。

【００４９】１．ｄｐ＝ｅ$^{-1}$（ｍｏｄ（ｐ－１））
２．ｄｐ＝ｅ$^{-1}$（ｍｏｄ（ｑ－１））
３．ｐ$^{-1}$（ｍｏｄ　ｑ）
４．ｐ^{0p}rimeおよびｑ^{0p}rime（Montgomery縮小 (reduction) のために使用される単一単位値）

値１～４はランダムに選択したＤＥＳキーＫを使用して暗号化され、暗号化されたデータはＲＡＭ１０４にストアされる。ハッシュ（例えば、ＭＤ５）は、少なくともＲＡＭ内のこのデータについて行われ、チェックサムＣが生成される。値ｐ，ｑ，ｅ，ＫおよびＣは安全保護された不揮発性ストレージ２０８にストアされる。チェックサムは安全保護されたストレージにストアされたデータ全体にわたって生成され、データに付加される。このようにして、データが相対的に安全度の低いＲＡＭ１０４に置かれていても、その保全性と機密性が保持されることになる。

【００５０】ＲＡＭ内のデータが利用される前に、不揮発性メモリ内の安全保護データ全体にわたってチェックサムがとられ、付加されているチェックサムと突合わせ検査される。これらのチェックサムが同一であれば、チェックサムＣが安全保護された不揮発性ストレージ２０８からアクセスされ、保全性チェックがＲＡＭデータについて行われる。つまり、ＲＡＭデータでハッシュが行われて、別のチェックサムＣ* が生成され、これは対応するチェックサムＣと比較される。この比較または以前の比較が失敗したときは、データは壊れているものとみなされ、安全保護データとＲＡＭ記憶データはデフォルト値にセットされる。これらのチェックサムが同一であれば、キーＫがアクセスされ、ＲＡＭデータが暗号解読され、利用されることになる。つまり、アイテム１～４がアクセスされ、私用キー暗号化で使用される。ＤＥＳ暗号化はスマート・カード２０によって行われるが、これは好ましい方法である。別の方法として、ＢＯＸに別の暗号化／暗号解読ハードウェアを含めることも可能であり、その場合は、このハードウェアがアクセスされてＲＡＭ内の値のＤＥＳ暗号化と暗号解読が行われることになる。

【００５１】上述した手法を使用すると、相対的に安全度の高い記憶媒体に格納された暗号キーを使用して情報を暗号化し、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアしておくことができるので、相対的に大量のセンシティブ情報を安全な状態で相対的に安全度の低い記憶媒体にストアしておくことができる。

【００５２】図５はマルチメディアまたはインタラクティブ・テレビジョン・レシーバをブロック図で示している。信号はアンテナ８０によって検出され、チューナ検出器８１に入力され、そこで受信信号の特定の周波数バンドが抽出され、ベースバンド多重化パケット信号が得

19

られる。周波数バンドは、システム・コントローラ８９（以下、ＩＲＤコントローラという）を通してユーザによって選択されるが、その方法は従来と同じである。公称的には、ブロードキャスト信号は、例えば、Reed-Solomon順方向エラー訂正(forward error correcting - ＦＥＣ）符号化を使用して、すでにエラー符号化されている。従って、ベースバンド信号はＦＥＣデコーダ８２に入力される。ＦＥＣデコーダ８２は受信ビデオを同期化し、定期的に、あるいは例えば、メモリ・コントローラ８７から要求があったとき、パケットを出力する。どちらの場合も、パケット・フレーム化または同期信号はＦＥＣ回路から得られ、それぞれのパケット情報がＦＥＣ８２から送出された回数を示している。

【００５３】単一プログラム信号からのパケットだけがレシーバによって処理される。この例では、多重化パケット・ストリームからどのパケットが選択されるかは、ユーザが知らないものと想定している。この情報はプログラム・ガイドに入っているが、このガイド自体もプログラムであり、それぞれのサービス・チャネルＩＤ、つまり、ＳＣＩＤを通してプログラム信号コンポーネントを相互に関係づけるデータからなっている。プログラム・ガイドは各プログラム別にリストしたもので、そこには、それぞれのプログラムのオーディオ、ビデオ、およびデータ・コンポーネントのＳＣＩＤが含まれている。プログラム・ガイドには、一定のＳＣＩＤが割り当てられている。レシーバに電源が入ったとき、ＩＲＤコントローラ８９はプログラム・ガイドに関連するＳＣＩＤをＳＣＩＤ検出器８４にロードするようにプログラムされている。なお、ＳＣＩＤ検出器は整合フィルタのバンクにすることができる。プログラム・ガイドＳＣＩＤが検出されると、メモリ・コントローラ８７は対応するパケット・ペイロードをメモリ８８内のあらかじめ決めたロケーションに送るように条件づけられており、これはＩＲＤコントローラによって使用される。

【００５４】ＩＲＤコントローラは、インタフェース９０を通してユーザからプログラミング・コマンドが送られてくるのを待っている。なお、インタフェースはキーボードが図示されているが、これは従来のリモート・コントロールにすることも、レシーバ・フロント・パネル・スイッチにすることも可能である。ユーザはチャネル４（アナログＴＶシステムで通常言われている用語）から送られてきたプログラムを見ることを要求したとする。ＩＲＤコントローラ８９は、チャネル４のプログラム・コンポーネントのそれぞれのＳＣＩＤ別にメモリ８８にロードされていたプログラム・ガイド・リストをスキャンし、これらのＳＣＩＤをＳＣＩＤ検出器８４にロードするようにプログラムされている。

【００５５】要求されたプログラムのオーディオ、ビデオまたはデータ・プログラム・コンポーネントの受信パケットは、最終的には、それぞれのオーディオ・プロセ

20

ッサ９３、ビデオ・プロセッサ９２、または補助データ信号プロセッサ９１（９４）へ送らなければならない。データは相対的に一定のレートで受信されるが、信号プロセッサは、公称的には、データがバーストで入力されることを要求している（ただし、例えば、圧縮復元（伸張）のそれぞれのタイプによる）。図５に例示するシステムでは、まず、それぞれのパケットはメモリ８８内のあらかじめ決めたメモリ・ロケーションへ送られる。そのあと、それぞれのプロセッサ９１～９４はコンポーネント・パケットをメモリ８８に要求する。コンポーネントをメモリ経由で送るようにすると、ある程度の望ましい信号データ・レートのバッファリングやスロットリングを行うことができる。

【００５６】オーディオ、ビデオおよびデータ・パケットはそれぞれのあらかじめ決めたメモリ・ロケーションにロードされ、各プロセッサがコンポーネント・データを容易にアクセスできるようにしている。それぞれのコンポーネント・パケットのペイロードは、対応するＳＣＩＤと、ＳＣＩＤ検出器から出された制御信号に応じて該当のメモリ・エリアにロードされる。この関連付けはメモリ・コントローラ８７にハードワイヤ(hardwired)することができるが、プログラマブルにすることも可能である。

【００５７】それぞれの信号パケットはＦＥＣ８２から信号デスクランブラ(signal descrambler)８６を経由してメモリ・コントローラ８７に結合されている。それぞれの信号パケットはヘッダとペイロードを含んでいる。信号ペイロードだけがスクランブルされ、パケット・ヘッダは未変更のままデスクランブラによってパスされる。パケットがデスクランブルされるかどうかはパケット・ヘッダのフラグによって決まり、パケットがどのようにデスクランブルされるかはパケット・ヘッダの二番目のフラグによって決まる。このパケット・デスクランブリングは、上述したアプリケーション・モジュール・セキュリティ処理からほぼ独立している。

【００５８】インタラクティブ・システムには、マルチメディア信号のデータ部分と共に動作できる複数のデバイスを含めることが可能である。例えば、図５において、ＡＵＸ１プロセッサとＡＵＸ２プロセッサはどちらも、信号のデータ部分に応答して動作するようになっている。ＡＵＸ１プロセッサは、送信株式市場データを検出し、そのデータを送信インタラクティブ・アプリケーションで操作するように構成されたパーソナル・コンピュータＰＣにすることができる。ＡＵＸ２は、送信インタラクティブ・コマーシャルと関連づけてインタラクティブな衝動買いができるように構成されたテレビジョン・システムにすることができる。なお、インタラクティブは、図５のシステムと相互接続された電話モデム（図示せず）を使用すると容易化される。さらに、ＩＲＤコントローラ８９は、特にシステム保守を目的に、送信ア

21

プリケーションを処理し、実行するようにプログラムすることが可能である。

【００５９】この例において上述したセンシティブ情報のストアはシステム・コントローラ８９によって行われるが、この例では、システム・コントローラはＲＯＭ、安全保護された不揮発性ストレージおよびスマート・カードを含んでいるものと想定している。ＲＡＭ１０４はメモリ８８のあらかじめ決めたブロックで構成することが可能である。ハードウェア・ドライバ４０８はメモリ・コントローラ８７に含まれている。この例では、図５に示すアイテムはすべてセット・トップ・ボックスに含まれている。

【図面の簡単な説明】

【図１】本発明を取り入れているインタラクティブ・テレビジョン・デコーダを示すブロック図である。

【図２】本発明を取り入れているセット・トップ・ボックスのオペレーションを、一部はブロック図で、一部はデータフロー図で示した図である。

22

【図３】本発明を取り入れているセット・トップ・ボックスのオペレーションを、一部はブロック図で、一部はデータフロー図で示した図である。

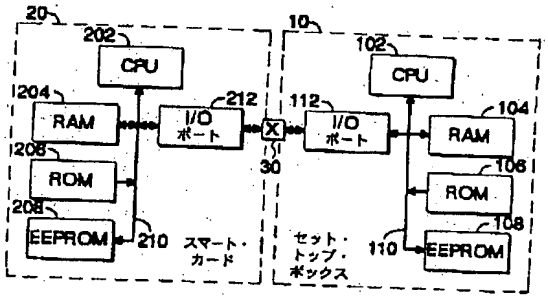
【図４】本発明を取り入れているセット・トップ・ボックスのオペレーションを、一部はブロック図で、一部はデータフロー図で示した図である。

【図５】本発明を実装できるレシーバを示すブロック図である。

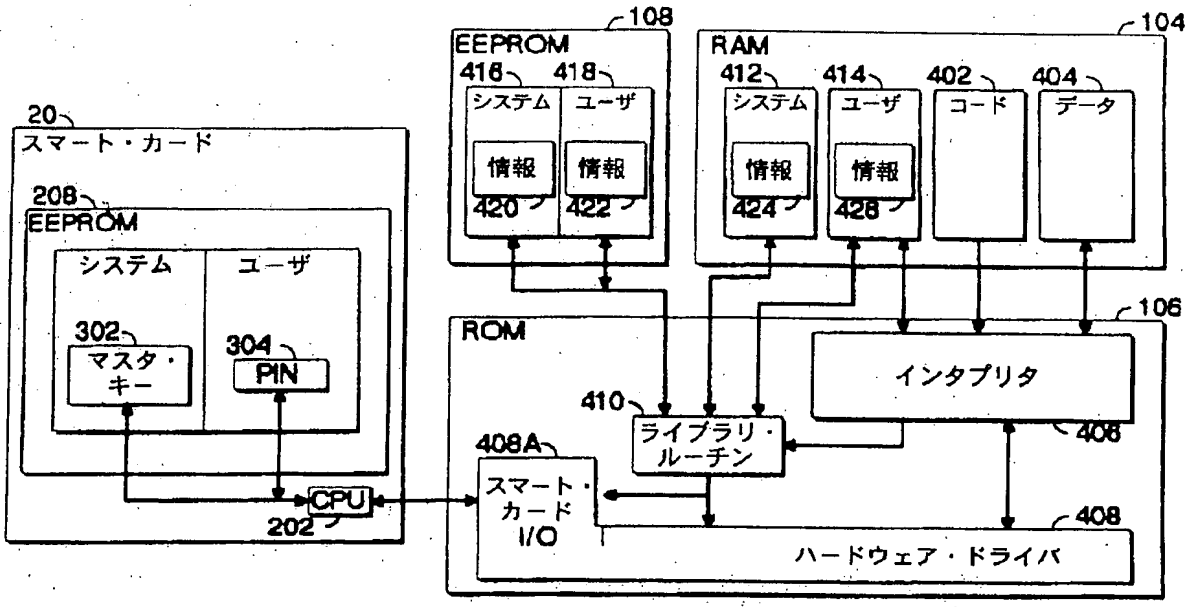
【符号の説明】

１０４　相対的に安全度の低い記憶媒体
１０８　相対的に安全度の低い記憶媒体
２０２　暗号化器
２０８　相対的に安全度の高い記憶媒体
３０２　暗号キー

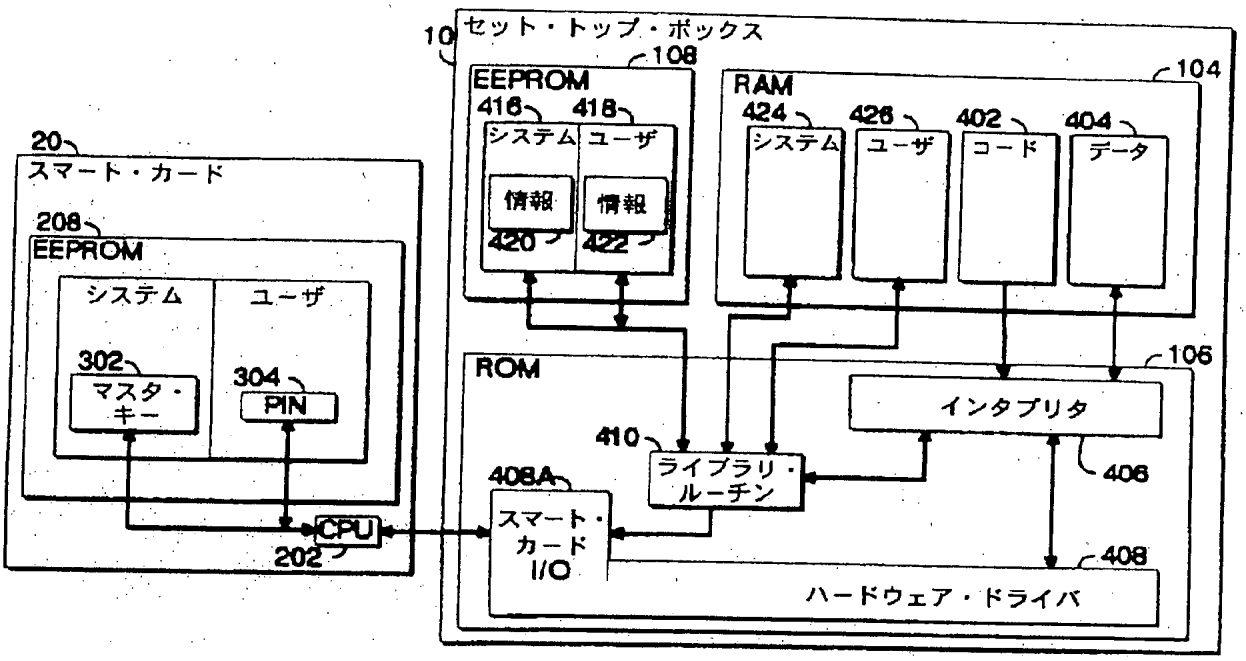
【図１】



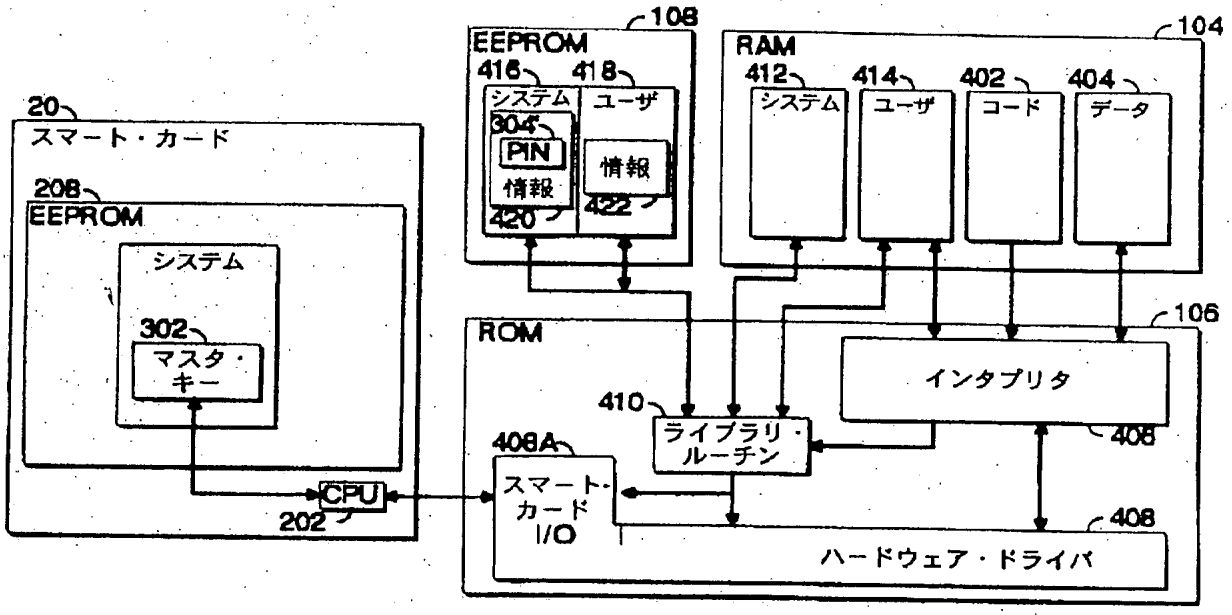
【図３】



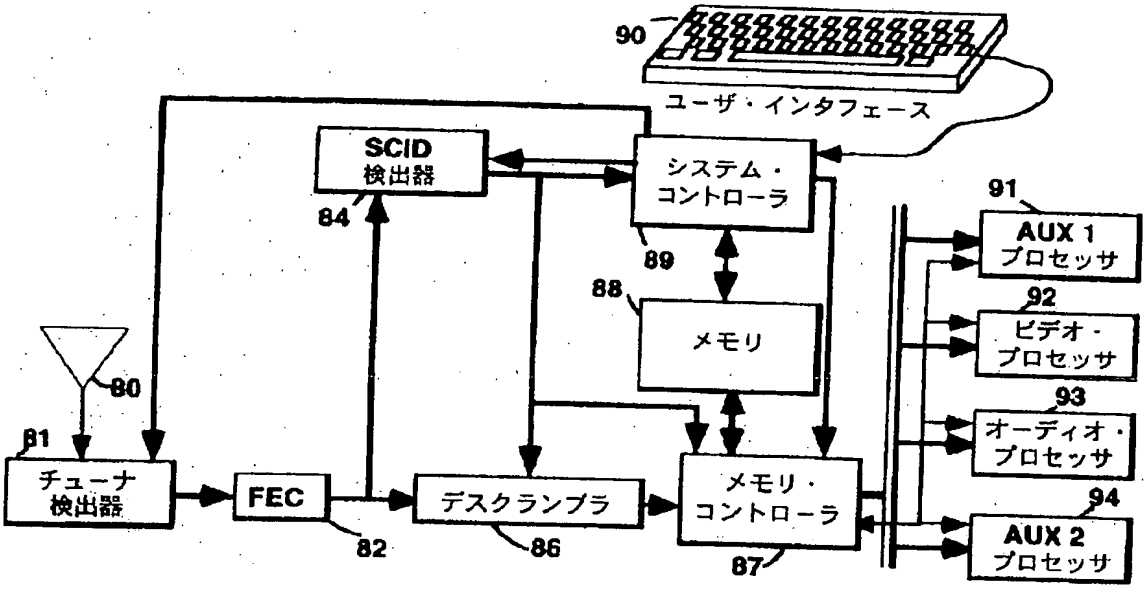
【図２】


10
セット・トップ・ボックス
108
EEPROM
416
418
システム
ユーザ
情報
情報
420
422
104
RAM
424
426
402
404
システム
ユーザ
コード
データ
20
スマート・カード
208
EEPROM
システム
ユーザ
302
マスタ・キー
304
PIN
106
ROM
インタプリタ
410
ライブラリ・ルーチン
406
408A
スマート・カードI/O
CPU
202
408
ハードウェア・ドライバ

【図４】


108
EEPROM
416
418
システム
ユーザ
304
PIN
情報
情報
420
422
104
RAM
412
414
402
404
システム
ユーザ
コード
データ
20
スマート・カード
208
EEPROM
システム
302
マスタ・キー
106
ROM
インタプリタ
410
ライブラリ・ルーチン
406
408A
スマート・カードI/O
CPU
202
408
ハードウェア・ドライバ

【図５】


90
ユーザ・インタフェース
SCID
検出器
84
システム・
コントローラ
89
91
AUX 1
プロセッサ
88
メモリ
92
ビデオ・
プロセッサ
80
93
オーディオ・
プロセッサ
81
チューナ
検出器
FEC
82
デスクランブラ
86
メモリ・
コントローラ
87
94
AUX 2
プロセッサ

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☑ SKEWED/SLANTED IMAGES
- ☑ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.